AFRL-IF-RS-TN-2006-4
Technical Note
March 2006

TRUST ARCHITECTURE FOR NETWORK KNOWLEDGE (TANK)

Trustees of the University of Pennsylvania

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. S523

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TN-2006-4 has been reviewed and is approved for publication.

APPROVED: /s/

ROBERT L. KAMINSKI
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	MARCH 2006	Final Tech Note, Jun 04 – Jun 05

4. TITLE AND SUBTITLE
TRUST ARCHITECTURE FOR NETWORK KNOWLEDGE (TANK)

5. FUNDING NUMBERS
C - FA8750-04-2-0241
PE - 62301E
PR - S523
TA - UP
WU - EN

6. AUTHOR(S)
MATTHEW A. BLAZE

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Trustees of the University of Pennsylvania
Office of Research Services
3451 Walnut Street, Room P221
Franklin Building
Philadelphia Pennsylvania 19104

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington Virginia 22203-1714

AFRL/IFGA
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TN-2006-4

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Robert L. Kaminski/IFGA/(315) 330-1867/ Robert.Kaminski@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

TANK used a DARPA-funded cognitive networking platform to demonstrate practical techniques for scalable mobile computing and also for practical distributed policy enforcement. Both results suggest new underpinnings for important DoD network environments such as ad-hoc tactical networks or multi-force battlefield networks.

14. SUBJECT TERMS
Cognitive networking, tactical networks, multi-force battlefield networks.

15. NUMBER OF PAGES
5

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Tank used a DARPA-funded cognitive networking platform to demonstrate practical techniques for scalable mobile computing and also for practical distributed policy enforcement. Both results suggest new underpinnings for important DoD network environments such as ad-hoctactical networks or multi-force battlefield networks.

The Trust Architecture for Network Knowledge (TANK) at the University of Pennsylvania demonstrated the value of trust management techniques in scalable mobile networking. We showed that a mobility solution can strictly outperform Mobile IP without sacrificing legacy interoperability. We also developed a novel system for detecting policy violations. Both of these new techniques are applicable to DoD networking, in one case in offering new flexibility to war fighters using mobile ad-hoc networks, and in another case showing new techniques for detecting compromised nodes in networks under heterogeneous control.

The core of TANK is a highly adaptive cognitive networking platform, DHARMA (Distributed Home Agent for Robust Mobile Access). DHARMA effectively and seamlessly circumvents the problem of intermittent connectivity/mobility on TCP applications that an increasingly important issue in mobile/wireless computing. Connectivity loss has received little attention because many major applications are not bothered by intermittent connectivity (e.g., Web browsing and email handling).

Inefficient routing in Mobile IP has been studied extensively, but DHARMA makes novel use of an overlay network to distribute Mobile IP home agent functionality to a collection of nodes. In particular, DHARMA selects a location-optimized instance from a distributed set of home agents to minimize routing overheads, and provides session support that overcomes both transitions between home agent instances and intermittent connectivity. Unlike Mobile IP and other network-layer mobility schemes, cross-layer information sharing between the session layer and the overlay network is used to exploit multiple (wireless) links when available.

We implemented DHARMA atop the PlantetLab testbed. Our results show that the routing performance of DHARMA is strictly better than best-case Mobile IP, and does not depend on continued bandwidth to a “home” network for mobile nodes. DHARMA’s routing performance improves with the number of proxies. In the PlanetLab Environment, with 10% proxy density, DHARMA’s routing overhead is 50% compared to standard TCP, while Mobile IP is 75% for triangular routing and 150% for bidirectional tunneling. With 100% proxy density nodes the routing overhead is reduced to 25%.

These results suggest a practical architecture for tactical networks, in which nodes obtain continued connectivity by exploiting highly varied network conditions without disturbing long-running applications (e.g., streaming multimedia).

A second aspect of TANK concerns evaluating the trustworthiness of nodes in large-scale networks, especially ad-hoc and peer-to-peer (P2P) systems. Such systems increasingly

distribute control to the end users, who may exploit characteristics of the system design to gain advantage; that is, they may engage in non-compliant behavior, more simply called policy violations or even “cheating”. Policy violations lead to poor performance, and can also indicate that a node has been compromised.

We also used network games as a testbed to study cheat detection in such networks; their complex and flexible protocol set, coupled with their large user base, provides a practical experimental environment that could be translated to other contexts. The researchers have formalized system invariants so that they can be represented in the knowledge base and allow accurate cheat detection. We showed that the invariants can be expressed in temporal logic. Moreover, the in-memory runtime check increases the average response time only by 0.21 milliseconds, and is unnoticeable by users. These results provide encouraging early evidence that distributed on-the-fly cheat detection may be feasible in practice in spite of the computation burden it places on peer nodes.

Distributed cheat detection is a promising approach in a variety of large-scale networks, especially ad-hoc networks made up of easily compromised nodes or those under heterogeneous control, such as multi-force battlefield networks.